511-CD-001-002

EOSDIS Core System Project

Release A Maintainability Demonstration Plan for the ECS Project

This document has not yet been approved by the Government for general use or distribution.

July 1996

Hughes Information Technology Systems
Upper Marlboro, Maryland

Release A Maintainability Demonstration Plan for theECS Project

July 1996

Prepared Under Contract NAS5-60000
CDRL Item #084

SUBMITTED BY

R. E. Clinard /s/	7/18/96
Robert Clinard, ECS CCB Chairman EOSDIS Core System Project	Date

Hughes Information Technology Systems
Upper Marlboro, Maryland

511-CD-001-002

This page intentionally left blank.

Preface

This document, as a formal contract deliverable with an approval code 1, required Government review and approval prior to acceptance and use. It was reviewed and approved, with comments, per GSFC Code 505 contracts letter dated November 7, 1995. Comments received with the approval letter have been incorporated, and this document is now considered accepted for use; no further review is required. Future changes to this document shall be made by document change notice (DCN) or by complete revision. Any future changes must be reviewed and approved by the Government.

This document is under ECS Project Configuration Control. Any questions or proposed changes should be addressed to:

Data Management Office
The ECS Project Office
Hughes Information Technology Systems
1616 McCormick Drive
Upper Marlboro, Maryland 20774-5372

This page intentionally left blank.

Abstract

The Maintainability Demonstration (MD) Plan presents the requirements and defined objectives for conducting MD tests of ECS Commercial Off-The-Shelf (COTS) hardware. The maintainability environment, maintenance approach for Release A, and system level Reliability, Maintainability, and Availability (RMA) requirements are discussed. The Plan outlines proposed failure scenarios for Release A and Flight Operations Segment (FOS) Release A/B that meet the defined MD objectives, and map directly to existing Acceptance test (AT) test cases.

Keywords: Maintainability, mean down time (MDT), failure, COTS, hardware, RMA, repair, fault, diagnostics, spares, maintenance

This page intentionally left blank.

Change Information Page

List of Effective Pages	
Page Number	**Issue**
Title	Submitted for TRR
iii through x	Submitted for TRR
1-1 through 1-2	Submitted for TRR
2-1 through 2-2	Submitted for TRR
3-1 through 3-4	Submitted for TRR
4-1 through 4-4	Submitted for TRR
A-1 through A-8	Submitted for TRR
AB-1 through AB-4	Submitted for TRR

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
511-CD-001-001	Original	Oct 1995	95-0738
511-CD-001-002	Submitted for TRR	July 1996	96-0731

This page intentionally left blank.

Contents

1. Introduction

2. Related Documentation

3. ECS Maintainability Environment

4. Maintainability Demonstration (MD) Process and Objectives

List of Tables

Appendix A: Failure Scenarios

Abbreviations and Acronyms

1. Introduction

1.1 Identification

This document, Contract Data Requirements List (CDRL) Item 084, whose requirements are specified in Data Item Description (DID) 511/PA1, is a required deliverable under the Earth Observing System Data and Information System (EOSDIS) Core System (ECS), Contract NAS5-60000.

1.2 Scope

This document applies to commercial off-the-shelf (COTS) hardware selected, procured, integrated and tested for an operational ECS Release. ECS is not planning to develop any custom hardware. This Plan does not apply to the maintainability of ECS developed or COTS software. This plan proposes Maintainability Demonstration (MD) failure scenarios that meet defined MD objectives. Candidate failure scenarios are mapped into existing Acceptance Test Cases. The ECS COTS hardware has been designed to commercial maintainability standards and support practices, and these MD scenarios do not verify unit level COTS Mean Time to Repair (MTTR) or commercial maintainability design. This document covers Release A and is being updated for TRR.

This document reflects the February 7, 1996 Technical Baseline maintained by the contractor Configuration Control Board (CCB) in accordance with ECS technical direction # 11, dated December 6, 1994.

1.3 Purpose

The MD Plan presents the requirements and defined objectives for conducting MD tests of ECS COTS hardware. The maintainability environment, maintenance approach for Release A, and system level RMA requirements are discussed. The Plan outlines proposed failure scenarios that meet the defined MD objectives, and map directly to existing Acceptance Test (AT) Test Cases described in the ECS Overall System Acceptance Test Plan for Release A (DID 409/VE1).

1.4 Status and Schedule

The original submission of this plan is due 2 weeks prior to the CDR for FOS and update 2 weeks prior to Rel A Test Readiness Review (TRR). The scenarios proposed will be detailed as MD Test Plans in DID 512, 2 weeks prior to Consent to Ship Review (CSR). These Test Plans will be coordinated with their corresponding Acceptance Test Procedures in DID 411, implementing the corresponding Acceptance Test Cases in DID 409.

1.5 Organization

The contents of this document are as follows:

- Section 1: Introduction - Introduces the Maintainability Demonstration Plan scope, purpose, schedule, and document organization.
- Section 2: Related Documentation - Describes the parent and applicable documents useful in understanding the details of subjects discussed in this document.
- Section 3: ECS Maintainability Environment - Discusses COTS hardware maintainability characteristics, Rel A operations and maintenance planning, and ECS system functional RMA requirements.
- Section 4: MD Process and Objectives - Describes the implementation process for this Plan, and the 3 MD objectives and how they are achieved.
- Appendix A: Failure Scenarios MD 1-4 for Release A, and Failure Scenarios MD 5-8 for Release B FOS.

2. Related Documentation

2.1 Parent Documents

The parent documents are the documents from which this Maintainability Demonstration Plan's scope and content are derived.

420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work
423-41-02	Goddard Space Fight Center, Functional and Performance Requirements Specification for the EOSDIS Core System (ECS)

2.2 Applicable Documents

The following documents are referenced within this Maintainability Demonstration Plan or are directly applicable, or contain policies or other directive matters that are binding upon the content of this document:

409-CD-001-004	ECS Overall System Acceptance Test Plan for Release A
517-CD-001-004	Failure Modes and Effects Analyses (FMEA) and Critical Items List (CIL) for the ECS Project
613-CD-002-001	Release A COTS Maintenance Plan for the ECS Project

This page intentionally left blank.

3. ECS Maintainability Environment

3.1 COTS Hardware

The ECS hardware for Rel A at Critical Design and for Rel B FOS is COTS, with no custom hardware or modified COTS planned or expected. The COTS hardware has been designed and built to commercial maintainability standards and practices. This characterizes the COTS hardware as:

a. Modular in design and fabrication

b. Designed to efficiently troubleshoot and maintain

c. Maintained by isolating to and replacing Line Replaceable Units (LRUs)

d. Typical Mean Time To Repair (MTTR) from 1/2 to 1 hour

e. Some level of vendor diagnostics will assist trouble shooting

f. No Preventive Maintenance normally required

g. No special tools or test equipment normally required

Most COTS hardware manufacturers offer warranty and extended warranty maintenance support for their products through their own service/support organizations. They are therefore motivated to design in maintainability to minimize their own support time and materiel costs. Their maintenance technicians are generally well trained, certified, and have access to sophisticated diagnostics and back-up help desks.

These COTS maintainability factors support an MD planning approach that assumes the inherent commercial maintainability of ECS COTS hardware, and does not require evaluating the maintainability design or demonstrating the MTTR of any unit level COTS hardware product.

3.2 ECS Maintenance and Operations

ECS operations will commence at Release Readiness Review. Release A operational hours for the Distributed Active Archive Centers (DAACs) will be in accordance with the schedules in the ECS Operations Plan, DID 608.

Once operations commence, COTS maintenance coverage to the DAACs, System Monitoring and Coordination Center (SMC), and EOS Operations Center (EOC) will be consistent with the operations requirements of ECS-supported missions (e.g. TRMM, Landsat 7, etc.). Because of the higher costs of maintenance support during extended operations hours (i.e. nights, weekends, and holidays), maintenance coverage during these periods will be limited to that required to sustain mission-critical operations and to satisfy ECS A_o and MDT requirements. Generally, the minimum principal period of maintenance (PPM) at the DAACs, EOC, SMC, and EDF will be 8AM to 5PM local, Monday through Friday, excluding local holidays.

Because of the low equipment quantities at the DAACs during Release A, full time maintenance engineers are not positioned at all sites. However, an on-site maintenance capability is provided by local maintenance coordinators (LMCs) to satisfy the operational availability and MDT requirements for some ECS functions (e.g. communications and science processing). Factors considered in the selection of COTS hardware (HW) to be maintained by LMCs include criticality of the equipment and redundancy of components/systems; technical expertise needed to diagnose and replace failed LRUs; and the cost of training, spares, and support equipment.

LMCs are trained and certified to perform maintenance on selected ECS equipment. Where the LMC has been designated as the principal maintenance provider for COTS HW and software (SW), his responsibilities include fault diagnostics and identification to the LRU level; replacement of failed LRUs with site spares; or escalating the problem to the responsible COTS contractor or the SMC for further assistance in diagnosing the cause of the problem.

When a COTS problem occurs, the LMC uses diagnostics tools, such as OpenView and built-in diagnostics, to identify and isolate the problem to the malfunctioning component, which may be SW or a failed LRU. If HW is identified as the source, the LMC or maintenance subcontractor corrects the problem by replacing the failed LRU with site spares, putting the unit back into operation, and testing the equipment and subsystem to verify the problem has been corrected.

Site engineering staffs and their LMC may be unable to resolve some of the more difficult maintenance problems. For this reason, backup support is available from a number of sources, including the SMC, Sustaining Engineering Organizations (SEO), maintenance subcontractors, and Original Equipment Manufacturers (OEMs). The LMC, following local procedures and ECS policy, determines if backup support is required based upon the nature of the problem. Network and SW-related problems may be referred to the SMC for assistance, while HW problems are normally referred to the local COTS hardware maintenance subcontractor for resolution.

3.3 Operational Availability (Ao) and Mean Down Time (MDT)

The ECS A_O and MDT requirements differ between the FOS, Science Data Processing Segment (SDPS), and Communications and Systems Management Segment (CSMS) functions, depending on the criticality of the function involved. The specific A_O and MDT objectives for the segments and functions within segments are stated in Section 5 of GSFC 423-41-02, Rev A, dated June 2, 1994, and are shown in Table 3-1 below, "ECS Operational Requirements." It is emphasized that these requirements do not apply to individual/unit level COTS hardware products, but rather apply to the entire system or sub-system function as indicated in the table.

Downtime has the greatest influence on achieving Ao in the mathematical relationship, and also is emphasized through its own MDT requirements. These are downtime averages (mean) across all COTS hardware failures in the functional string over a period of time. When averaging multiple failures, those with long downtime delays can be offset by short downtime switchover corrected failures in the computation of MDT. The MDT requirement is not a discrete amount of time allowed for each individual failure, and should not be measured or demonstrated as such.

Table 3-1. ECS Operational

ECS Function	Functions	A_O Minimum	MDT Maximum
	Flight Operations Segment (FOS)		
3800	Critical Real-time Functions*	0.9998	1 Min.
3810	Non-Critical Real-time Functions*	0.99925	5 Min.
3820	Targets of Opportunity (TOO) *	0.992	1 Hr
3700	ECS Functions not Otherwise Specified	0.96	4 Hrs
3710	ECS shall have no single point of failure for functions associated with real time operations of the spacecraft and instruments		
	Science Data Processing Segment (SDPS)		
3900	Science Data Receiving	0.999	2 Hrs
3910	Switch over from Primary Science Data Receipt to Backup	NA	15 Min. maximum
3920	Archiving & Distributing Data	0.98	2 Hrs
3930	User Interfaces to IMS Services at DAACs	0.993	2 Hrs
3940	Information Searches on the ECS Directory	0.993	2 Hrs
3950	Data Acquisition Request Submittals including TOOs*	0.993	2 Hrs
3960	Metadata Ingest and Update	0.96	4 Hrs
3970	Information Searches on Local Holdings	0.96	4 Hrs
3980	Local Data Order Submission	0.96	4 Hrs
3990	Data Order Submission Across DAACs	0.96	4 Hrs
4000	IMS Data Base Management and Maintenance Interface	0.96	4 Hrs
4010	Product Generation Computers	0.95	NA
4020	Product generation computers shall provide a "Fail soft" environment		
	Communications and System Monitoring Segment (CSMS)		
4030	SMC functions of Gathering and Disseminating System Management Information	0.998	20 Min.
4035	ESN shall have no single point of failure for functions associated with network databases and configuration data		
4036	ESN A_O shall be consistent with the specified A_O of the ECS functions.		
3630	Maximum down time shall not exceed twice the required MDT in 99 percent of failure occurrences		

A_O = Operational Availability

MDT= Mean Down Time

* = Required for Release B and subsequent releases only (all other functions required for Release A and subsequent releases)

This page intentionally left blank.

4. Maintainability Demonstration (MD) Process and Objectives

4.1 Process

The EOS Performance Assurance Requirements for the ECS, GSFC 420-05-03, in RMA section 5.6 presents the MD process and objectives. In accordance with this guidance and consistent with DID 511 this Plan outlines proposed failure scenarios that achieve the MD objectives. These scenarios are to be reviewed by the Independent Acceptance Test Organization (IATO) and those selected conducted as part of the Acceptance Test (AT) program. The proposed failure scenarios have been mapped to existing AT test cases with similar objectives. It is appropriate to consider combining AT test cases and MD scenarios with the same objectives into one test case, rather than accomplishing redundant tests.

A high level failure analysis was performed during the development of the failure scenarios. Hardware failure rates were considered in the form of vendor provided COTS Reliability Predictions. The in-service failure history of COTS products operating in the EDF was also reviewed and considered. The EDF COTS are representative of Release A and have been under OEM warranty and third party maintenance provider support.

A Failure Modes and Effects Analysis (FMEA) has been conducted on the FOS Critical Real-Time functions. Thirty-five LRUs and 123 failure modes were identified and all are Criticality 4 classifications. This means that all identified failures of the FOS Critical Real-Time functions will not impact the science mission due to the FOS robust design with its extensive redundant hardware architecture. This also confirmed that there is no single point of failure.

4.2 MD Objectives

The Performance Assurance Requirements (PAR) Section 5.6 and DID 511 establish three objectives for the Maintainability Demonstrations. These are discussed below and related to the specific MD failure scenarios proposed in Appendix A.

4.2.1 Verify Capability to Meet Ao and MDT

"The objective of the demonstrations is to verify the capability of the planned maintenance activities to meet the operational availability/mean down times stated in the ECS F&P Specification for identified system functions." The PAR Section 5.6 identifies the system functions as the critical real-time system functions (primarily in the FOS).

As discussed in Section 3.3, the F&P specification RMA requirements are system function requirements applying across all the COTS hardware implementing that function. An MD test is normally accomplished on one individual unit level COTS product; any resulting downtime measure would not represent all the COTS hardware in the function for the given time period. Also, Ao is not directly measurable through an MD test; the principal component downtime, however, is.

Since critical real-time system functions are specified and exist only in the FOS, and since the MDT requirements for these are 1 minute or less they are only achievable through hardware redundancy in the design and software switchover in the event of failure. This switchover is demonstrable through MD tests and will achieve this MD objective. Failure scenarios to demonstrate switchover are proposed for the FOS critical real-time functions during Rel B. These are included in Appendix A as scenarios MD - 5, 6, 7, and 8 during Rel B. The failures in these scenarios are the most probable anticipated failures in the FOS hardware architecture.

In all the scenarios, it is not intended to demonstrate the mean of MDT through a sample size and series of tests, but rather the capability to achieve MDT during operations. This can be demonstrated in one MD test for each scenario by accomplishing failover or switchover within the required time and comparing this test result to previous demonstrations, integration, and system test results in the test report.

FOS Critical Command and Control Systems are systems that provide critical real-time functions to support the following: launch, early orbit checkout, disposal, orbit adjustment, anomaly investigation, recovery from safe mode, routine real-time commanding and associated monitoring for spacecraft and instrument health and safety. This includes the execution and control of the ground script; the uplink of spacecraft loads, instrument loads and real-time commands; command verification; ingest and monitoring of the real-time housekeeping telemetry and replay telemetry; and the capture and recording of real-time deviations to the planned ground script to ensure that the as-flown ground script is accurate.

For Release A/B, the FOS Critical Command and Control Systems that perform critical real-time functions consist of redundant groups of Real-Time Servers, Data Servers (for Events archiving function only), User Stations, RAID (Redundant Array of Independent Disks) storage devices, Time Systems, and network equipment (concentrators and hub/bridge assemblies).

4.2.2 Evaluate Fault Detection/Isolation Methods

The Management Subsystem (MSS) Fault Management Application Service will be implemented in Release A and will be demonstrated in each of the proposed failure scenarios as the primary fault detection capability. Alerts and reports will initiate further fault/failure isolation and subsequent trouble shooting using COTS diagnostic tools as appropriate. All the proposed failure scenarios 1-8 will evaluate this fault detection objective.

4.2.3 Evaluate Ability to Achieve LRU Replacements On-site

The intent of this objective is to conduct a non-quantified evaluation of the on-site maintenance capability, consistent with the COTS Maintenance plan. An analysis of the COTS maintenance processes to be implemented during Rel A on-site and evaluation of the training, certification, and proficiency of assigned personnel will achieve this objective. Additionally a review and analysis of the COTS hardware failure activities in the EDF over the last 2 years will provide assessment of the vendor OEM and third party maintenance processes in effect. The vendor response times effective for the EDF are not as stringent as will be required for on-site operations. No MD failure scenario specific to these maintenance process evaluations is proposed.

Failure scenario MD -4 Network Failure Recovery will be constructed to require the hot swapping of network communications device LRUs to achieve failure recovery. Release A COTS will be under warranty during the AT period, and a COTS HW failure after detection, isolation, and confirmation of hardware failure will be corrected on-site by the OEM warranty vendor. This unplanned, unrehearsed failure activity will also provide a demonstration and assessment of this maintenance approach.

The fault detection activities, operator response, local maintenance coordinator diagnosis and fault isolation process, OEM vendor contact and support, LRU identification and changeout, vendor spares positioning and availability, corrective action verification, and maintenance data collection can all be observed and analyzed as unplanned and unrehearsed actions. This unscheduled opportunity provides a demonstration of real failure OEM corrective action processes at the local site level.

This page intentionally left blank.

Appendix A: Failure Scenarios

A.1 Evaluate Management SubSystem (MSS) Fault Management Application Service

Test No.: MD - 1 Rel A

AT Test Case: A080610.030-System and Site Fault Diagnostic Testing

Test Title: Evaluate Management SubSystem (MSS) Fault Management Application Service

Failure Scenario Description:

This test is designed to evaluate the capability, effectiveness, and useability of the Fault Management Service to detect, document, diagnose, isolate, provide impact status and assessment, and facilitate recovery from faults. The evaluation will be in the context of normal ECS on-site operations being interrupted by planned hardware fault events or simulations with the focus on the effectiveness of this service in identifying and facilitating the accomplishment of corrective actions at the local site level. Local operator and local maintenance coordinator interactions with the service and its responsiveness and useability will be evaluated.

Input: Standard ECS site operating environment; MD test plans for specific HW failures; manual disconnection of the HW to simulate a failure, or introduction of real component failure.

Output:

Configuration status and fault event message displays/printouts; generated datasets.

Success Criteria:

Following HW failure, operators receive Fault error messages detecting and isolating failure to the specific COTS HW. Appropriate diagnostics can be executed to further diagnose the specific hardware fault and/or failed LRU. The Fault Management Service facilitates and assists the user, operator, local maintenance coordinator, or system administrator in specifying and accomplishing the corrective action required. The service facilitates and enhances operator corrective action decision processes with accurate, useful operational status; recovery alternatives if available; and failure impacts to operations processes and data. Configuration display pages accurately portray the HW configuration before, during, and after the HW failure.

A.2 MSS Critical Services Failure Recovery

Test No.: MD - 2 Rel A

AT Test Case : A080510.030-RMA Assurance Test and Analysis

Test Title: MSS Critical Services Failure Recovery

Failure Scenario Description:

This test evaluates the failover design of the server providing the MSS Critical Services in meeting the MSS function RMA MDT requirement of 20 minutes or less. A fault event in the server is simulated or a planned component failure is introduced to create the failure. The Fault Management Application Service will detect the failure and local operator/administrator action will be taken to diagnose, isolate the failure and initiate recovery corrective action. These diagnostic actions, switchover to the Failover server, and resumption of full Critical MSS Services should be completed within 20 minutes.

Input: Standard ECS site operating environment; MD test plan for the specific HW failure; manual disconnection of the HW to simulate a failure, or introduction of real component failure.

Output:

Configuration status and fault event message displays/printouts; generated datasets.

Success Criteria:

Following HW failure, operators receive Fault error messages detecting and isolating failure to the specific MSS Server. Appropriate diagnostics can be executed to further diagnose the specific hardware fault and/or failed LRU. Fault Management facilitates and assists the operator, local maintenance coordinator, or system administrator in specifying and accomplishing the corrective action required. These diagnostic actions, switchover to the Failover MSS Server, and resumption of full Critical MSS Services will be completed within 20 minutes. Configuration display pages accurately portray the HW configuration before, during, and after the HW failure.

A.3 Primary Science Data Receipt Capability Failure Recovery

Test No.: MD - 3 Rel A

AT Test Case : A080510.030-RMA Assurance Test and Analysis

Test Title: Primary Science Data Receipt Capability Failure Recovery

Failure Scenario Description:

This test evaluates the failover design of the Ingest server providing the primary science data receipt capability to meet the RMA function switchover time requirement of 15 minutes or less. A fault event in the Ingest server is simulated or a planned component failure is introduced to create the failure. The Fault Management Application Service will detect the failure and local operator/administrator action will be taken to diagnose and isolate the failure and initiate recovery corrective action. These diagnostic actions, switchover time to the failover server, and resumption of full science data receipt services should be completed within 15 minutes.

Input: Standard ECS site operating environment; MD test plan for the specific HW failure; manual disconnection of the HW to simulate a failure, or introduction of real component failure.

Output:

Configuration status and fault event message displays/printouts; generated datasets.

Success Criteria:

Following HW failure, operators receive Fault error messages detecting and isolating failure to the specific Ingest Server. Appropriate diagnostics can be executed to further diagnose the specific hardware fault and/or failed LRU. Fault Management facilitates and assists the operator, local maintenance coordinator, or system administrator in specifying and accomplishing the corrective action required. These diagnostic actions, switchover time to the failover server, and resumption of full Science Data Receipt Capability will be completed within 15 minutes. Configuration display pages accurately portray the HW configuration before, during, and after the HW failure.

A.4 Network Failure Recovery

Test No.: MD - 4 Rel A

AT Test Case: A080490.070-Network Fault Management

Test Title: Network Failure Recovery

Failure Scenario Description:

This test evaluates both the network's ability to detect, diagnose, analyze, and report network faults and errors, at both the local site and SMC levels, and also the local maintenance coordinator's responsiveness in taking appropriate corrective action. A network failure is simulated or a real component failure is introduced in a network hardware device. The fault management capability will detect the failure and facilitate isolation to the device and the diagnosis of the problem. Appropriate reports and alerts will be generated. Since the COTS network hardware device is designed with hot swappable components the failure will evaluate the local site's effectiveness in accomplishing the needed hot swap using available component LRUs. The hot swap can either be simulated or accomplished. The network will be maintained in normal operational status.

Input: Standard ECS site operating environment; MD test plan for the specific network hardware device failure; manual disconnection of the HW to simulate a failure, or introduction of real component failure.

Output:

Configuration status and fault event message displays/printouts; generated datasets.

Success Criteria:

Following network device failure, operators receive fault error messages detecting and isolating failure to the specific device. The network has remained operational with no data loss. Appropriate diagnostics can be executed to further diagnose the specific hardware fault and/or failed LRU. Fault Management facilitates and assists the operator, local maintenance coordinator, or system administrator in specifying and accomplishing the corrective action required. If this test is a real hot swappable component failure, the changeout of the LRU is accomplished using on-site spares.

Configuration display pages accurately portray the HW configuration before, during, and after the HW failure.

A.5 FOS Network Fault Recovery

Test No.: MD - 5 Rel B

AT Test Case: B080620.020-Network Fault Management

B110210.080-FOS Fault Processing/Equipment Failover

Test Title: FOS Network Fault Recovery

Failure Scenario Description:

This test is designed to verify the capability of recovering from failures of network components supporting FOS operations, including the Operational LAN (FDDI-Fibre Distributed Data Interface) within a down time of one minute or less, and also Ethernet and hub failures, EOSDIS Backbone Network (EBnet) Router failure and EOC router failure.

The test begins with the sign-on of several user stations and the initialization of the EOC. Configuration and event pages are displayed and used to verify the EOC configuration following logical string assignments and reconfiguration activity performed by the user with ground configuration authority. Logical string assignments supporting real-time, simulation and replay strings are performed for each supported mode (i.e. operational, test, and training). Following string assignments, each type of failure listed above is performed sequentially, with test steps included to ensure the recovery from each failure.

During recovery operations, alphanumeric display pages showing the FOS configuration components and status are viewed and printed at specified times (i.e. before, during, and after failure recovery) in order to verify the accurate representation of configuration information throughout the recovery period.

Input:

ECL directives for initializing the EOC; manual disassembling/disabling/disconnecting connected network components to simulate network/hub failures or to introduce real component failures.

Output:

Configuration status display pages/printouts and event displays/printouts at EOC/IST-Instrument Support Terminal user stations.

Success Criteria:

Following FDDI and FDDI hub failures, FDDI ring or hub wraps autonomously with no data loss and FOS software applications continue as normal, **and occurs within one minute**. During Ethernet failure, the EOC user stations on the Ethernet link lose connection to supported logical strings; the affected user station(s) successfully re-establishes former string connection on another EOC user station. Following an EBnet router failure, FOS receives event messages concerning

the failure and reconnection; no FOS configuration is required following recovery. Following EOC router failure and recovery, no FOS reconfiguration is required; IST user stations, following ECS Command Language (ECL) directives to reconnect to established logical strings, are successful in connecting. Upon any network failure, connected EOC/IST user stations receive error messages concerning the failure, and messages following network recovery. Configuration display pages accurately portray the FOS configuration before, during and after network failures.

A.6 FOS Real-time Server Failure Recovery

Test No.: MD - 6 Rel B

AT Test Case: B110210.080

Test Title: FOS Real-time Server Failure Recovery

Failure Scenario Description:

This test is designed to verify the capability of recovering from a real-time server failure during real-time operations within a down time of one minute or less.

The test begins with the sign-on of several user stations and the initialization of the EOC, including establishment of logical and backup strings, execution of the ground script, and the receipt of real-time telemetry. The real-time server is disconnected/powered down to simulate a failure, or a prepared component failure is introduced. Upon detecting telemetry data dropout and other event messages at connected EOC and IST user stations, the ground controller enters directives to transfer control to the backup, specifies the real-time server that is to receive control, and specifies if checkpoint information (telemetry and command path information) is to be applied. As the backup logical string is converted to active, the ground controller requests command authority, resumes the ground script and begins processing real-time telemetry.

Input:

ECL directives for initializing the EOC; manual disassembling/disabling/disconnecting real-time server to simulate server failure, or introduce real component failure.

Output:

Configuration status and event message displays/printouts.

Success Criteria:

Following server failure, EOC/ISTs receive event messages stating real-time data dropout, pause of the ground schedule, and server failure events. Request of ground configuration authority is granted following failure of the server. Directives to transfer control to the backup real-time server, and transfer checkpoint information are successful **and occur within one minute of request.** Previously running ground script resumes upon ECL directives. EOC/IST users connected to the failed real-time server are re-established to previous logical strings upon re-issue of connection directives. Configuration display pages accurately portray the FOS configuration before, during and after the real-time server failure.

A.7 FOS Data Server Failure Recovery

Test No.: MD - 7 Rel B

AT Test Case: B110210.080

Test Title: FOS Data Server Failure Recovery

Failure Scenario Description:

This test is designed to verify the capability of recovering from a data server failure during real-time operations within a down time of one minute or less.

The test begins with the sign-on of several user stations and the initialization of the EOC, including establishment of logical and backup strings. Several analysis requests for datasets are generated and submitted. During execution of the datasets, the data server is disconnected/ powered down to simulate a failure, or a prepared component failure is introduced. Upon detecting event messages stating communications failure with the data server appropriate corrective actions are taken. Configuration display pages are printed before, during and after failure recovery to ensure accurate portrayal of the FOS equipment configuration.

Input:

ECL directives for initializing the EOC; manual disconnection of the data server to simulate a failure, or introduction of real component failure.

Output:

Configuration status and event message displays/printouts; generated datasets.

Success Criteria:

Following server failure, EOC/ISTs receive error messages stating communications failure of the data server. Directives to transfer dataset generation to the backup data server result in the datasets generated without error. EOC/IST users connected to the failed real-time server are re-established to previous logical strings upon re-issue of connection directives; **this occurs within one minute.** Configuration display pages accurately portray the FOS configuration before, during and after the data server failure.

A.8 FOS User Station Failure Recovery

Test No.: MD - 8 Rel B

AT Test Case: B110210.080

Test Title: FOS User Station Failure Recovery

Failure Scenario Description:

This test is designed to verify the capability of recovering from a user station failure during real-time operations within a down time of one minute or less.

The test begins with the sign-on of several user stations and the initialization of the EOC, including establishment of logical and backup strings, execution of the ground script, and the receipt of real-time telemetry. The EOC user station currently operating as the ground controller/command issuer is disconnected/powered down to simulate a failure, or a real prepared component failure is introduced. Upon detecting the failure, the ground controller transfers to another EOC user station, requests command authority, applies checkpoint information to the ground script and resumes the script. Steps are also provided to ensure failure recovery from an IST user station failure.

Input:

ECL directives for initializing the EOC; manually disconnecting the user station to simulate a failure or introduction of component failure.

Output:

Configuration status and event message displays/printouts.

Success Criteria:

Request of ground configuration authority, transfer of checkpoint files to the ground script, and resumption of the ground script is successful following the issuance of the directives from another EOC user station **within a down time of one minute or less.** Configuration display pages accurately portray the FOS equipment configuration before, during and after the user station failure. IST users experiencing failure conditions may sign-on to another IST user station, and perform functions mirroring their previous activity on the failed user station.

This page intentionally left blank.

Abbreviations and Acronyms

A_o	Operational Availability
ASF	University of Alaska Synthetic Aperture Radar (SAR) Facility
CCB	Configuration Control Board
CDR	Critical Design Review
CDRD	Contract Data Requirement Document
CDRL	Contract Data Requirements List
CM	Configuration Management
COTS	Commercial Off-the-Shelf
CSMS	Communications and Systems Management Segment
CSS	Communications subsystem
DAACs	Distributed Active Archive Centers
DCN	Document Change Notice
DID	Data Item Description
DM	Data Management
EBNet	EOSDIS Backbone Network
ECL	ECS Command Language
ECS	EOSDIS Core System
EDC	Earth Resources Observation Systems (EROS) Data Center
EDF	ECS Development Facility
EOC	EOS Operations Center
EOS	Earth Observing System
EOSDIS	Earth Observing System (EOS) Data and Information System (DIS)
EROS	Earth Resources Observation Systems
ESD	Electrostatic Discharge
ESDIS	Earth Science Data and Information System
ESN	EOSDIS Science Network

FDDI	Fiber-optic Distributed Data Interface
FMEA	Failure Modes, and Effects Analyses
FOS	Flight Operations Segment
GFSC	Goddard Space Flight Center
HW	Hardware
IATO	Independent Acceptance Test Organization
IDR	Increment Design Review
ILS	Integrated Logistics Support
ILSO	ILS Office
IMS	Information Management System
ISS	Internetworking Subsystem
IST	Instrument Support Terminal
JPL	Jet Propulsion Laboratory
LaRC	Langley Research Center
LMC	Local Maintenance Coordinator
LORA	Level of Repair Analysis
LRU	Line Replaceable Unit
LSA	Logistics Support Analysis
M&O	Maintenance and Operations
MD	Maintainability Demonstration
MDT	Mean Down Time
MR	Malfunction Report
MSFC	Marshall Space Flight Center
MSS	Management Subsystem
MTTR	Mean Time To Repair
NA	Network Administrator
NASA	National Aeronautics and Space Administration
NSIDC	University of Colorado, National Snow and Ice Data Center
OEM	Original Equipment Manufacturer

OPPM	Outside PPM Hours
ORNL	Oak Ridge National Laboratory
PAIP	Performance Assurance Implementation Plan
PHS&T	Packaging, Handling, Storage, and Transportation
PM	Preventive Maintenance
PPM	Principal Period of Maintenance
RAID	Redundant Array of Independent Disks
RMA	Reliability, Maintainability, and Availability
SA	System Administrator
SAR	University of Alaska Synthetic Aperture Radar
SDPS	Science Data Processing Segment
SEO	Sustaining Engineering Organization
SMC	System Monitoring and Coordination Center
SOW	Statement of Work
SW	Software
TOO	Target Of Opportunity
TRR	Test Readiness Review
UPS	Uninterruptable Power Supply

This page intentionally left blank.